IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

RACHELLE RAND, ESPERANZA GOTTSCHAU, and RAMON SOTO on Behalf of Themselves and All Others Similarly Situated **Plaintiffs,** **v.** **EYEMART EXPRESS, LLC,** **Defendant.**	**Case No. 3:24-cv-00621**

DEFENDANT EYEMART EXPRESS, LLC'S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Defendant Eyemart Express LLC ("Eyemart") respectfully moves this Court to dismiss this action pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6).

I. SUMMARY OF ARGUMENT

Plaintiffs are all subscribers of Facebook, one of the many popular social media websites owned and operated by Meta Platforms, Inc. ("Meta"). When Plaintiffs signed up for Facebook, they struck a bargain: in exchange for free online services from Meta, Plaintiffs agreed to have certain online activities tracked by Meta for advertising purposes. Meta, in turn, provides a tool, the Meta Pixel, for businesses that advertise on Meta to install on their websites to better connect with their website visitors who are also Facebook subscribers. Plaintiffs, like all Facebook subscribers, are informed of these capabilities and functionalities from the outset of their subscriber relationship with Facebook. This is a voluntary, mutually beneficial, at-will arrangement. Facebook subscribers have control over when and how their online activities are tracked and used, and can opt-out at any time.

Plaintiffs admit all these basic, well-understood facts but now seek damages against Eyemart for Eyemart sending information to Meta which Plaintiffs affirmatively, actively, and continuously agreed with Meta to allow to be sent. Plaintiffs rely on nearly forty-year-old wiretapping laws, enacted before virtually any website existed, as the basis for their claimed damages. Plaintiffs' claims are not supported by the facts or the law and should be dismissed in their entirety for a multitude of reasons.

First, Plaintiffs lack standing—they have failed to plead any plausible factual basis for how they have been damaged by the alleged disclosure of public website browsing to Meta. As courts across the country are increasingly ruling in similar cases, an individual's activities which could be observed in a physical store are not transformed into a damaging violation of the individual's privacy when observed in a virtual store.

Additionally, Plaintiffs fail to state a claim and dismissal is required under Rule 12(b)(6). To the extent Plaintiffs' interactions with the Eyemart Website can be deemed "communications" under applicable law, those were "communications" from Plaintiffs to Eyemart, and Eyemart cannot "eavesdrop" on itself by accessing those communications. Eyemart consented to those "communications" being subsequently sent to Meta for the benefit of Meta, Eyemart, and the Facebook users like Plaintiffs who also consented to that sharing of information. The fact that Eyemart may be a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA") for some of the products and services Eyemart offers does not change the analysis. HIPAA does not provide for a private right of action, and there can be no good faith argument that Eyemart sent website information to Meta for the purpose of violating HIPAA rather than for the purpose of selling more Eyemart products and services to users interested in those products and services.

Even if the 1980s era wiretapping laws cited by Plaintiffs *were* applicable, the Complaint fails to provide a plausible factual basis for their applicability. Those laws require the interception of communications to be instantaneous, as in the example of a "wiretap" on a telecommunication line. Plaintiffs' allegations of "near instantaneous" transmission of their "communications" to Meta is an acknowledgement of their failure to meet that requirement.

Plaintiffs' contract claims fare no better. Plaintiffs consented to Meta and Eyemart sharing the type of data which Plaintiffs now object to. Plaintiffs fail to point to any express or implied contractual terms to the contrary.

Finally, Plaintiffs' claims under Illinois law and for "intrusion upon seclusion" fail to withstand scrutiny. Plaintiffs' allegations that the data sharing at issue was done "surreptitiously" or was of a type as to be so "highly offensive" as to intrude upon Plaintiffs' privacy are entirely

without merit. Plaintiffs' cited exemplars of "highly offensive" information sharing includes: (1) searching for Nike sunglasses on a public website and (2) locating eyewear store locations on a public website. This information sharing is simply not "highly offensive" under any colorable understanding of that term. Information sharing which is disclosed by both Eyemart and Meta (through policies and terms Plaintiffs agreed to) is publicly disclosed, readily available, and of a type which internet users have grown to understand and expect due to the regular and transparent nature of this type of information sharing across the world wide web.

In sum, Plaintiffs opted-in to using the internet in a certain way for Plaintiffs' convenience and now seek damages from Eyemart for Plaintiffs' own decisions. While there may be situations where website usage monitoring exceeds agreed to limits or applicable law, the instant case involving a public website operator tracking its Website usage through a popular, common, and agreed to social media provider is not that case. Plaintiffs' feigned surprise and outrage and attendant "injuries" and "damages" are unsupported by their own factual allegations and the law. Their claims should be dismissed for lack of standing and for failure to state a claim upon which relief can be granted.

II. FACTUAL BACKGROUND[1]

A. Summary of Plaintiffs' Allegations

[1] Plaintiffs' Complaint includes 79 footnotes and numerous citations to extrinsic materials. Under the doctrine of "incorporation by reference," a district court may look beyond the pleadings at certain materials—documents attached to the complaint, documents incorporated by reference in the complaint, or matters of judicial notice—without converting a Rule 12(b)(6) motion into one for summary judgment. *See* James W. Moore *et al.*, Moore's Federal Practice § 12.34[2] (3d ed. 1999); *Petrobras Am., Inc. v. Samsung Heavy Indus. Co., Ltd.*, 9 F.4th 247, 252 n.2 (5th Cir. 2021) (citing *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322, 127 S.Ct. 2499, 168 L.Ed.2d 179 (2007)). To the extent this Memorandum references documents incorporated by reference into the Complaint, Eyemart submits such documents are part of the Complaint under these principles.

Plaintiffs Rochelle Rand, Esperanza Gottschau, and Ramon Soto filed the instant action against Eyemart alleging injury as a result of the Eyemart website's (the "Website") use of the Meta Pixel on certain sections of that Website. Compl., Dkt. #1, at ¶¶ 1-4. Plaintiffs bring claims for violations of the Federal Wiretap Act (Count I), the Missouri Wiretap Act (Count II), the Illinois Eavesdropping Act (Count III), Intrusion Upon Seclusion (Count IV), Breach of Implied Contract (Count V), and Breach of Contract (Count VI).

B. Eyemart's Business and Website

Eyemart operates a chain of retail locations which sell eyeglasses, contact lenses, and sunglasses and related services. *Id*. at ¶ 28.[2] Eyemart also operates the Website which individuals can use to search for products and services which can be purchased from Eyemart stores. *Id.* at ¶ 1. The Website also provides methods to connect individuals to local Eyemart stores, such as to answer questions, plan on-site shopping, or to schedule an appointment with a salesperson or eyecare professional. *Id.* When an individual wishes to schedule an eye exam, that individual is provided either a phone number to schedule an appointment or is directed to the website of that eye exam provider to schedule such an appointment.[3]

C. Plaintiffs' Use of the Eyemart Website and Facebook

According to the Complaint, Rand accessed the Website in November of 2023 to search for an eye doctor, Gottschau accessed the Website in October of 2023 to search for prescription

[2] These non-conclusory facts are presented as alleged in the Complaint and are deemed true for purposes of a Rule 12 Motion to Dismiss, except where such factual allegations are contradicted by documents incorporated into the Complaint by reference. *See Doe v. Univ. of Tex. M.D. Anderson Cancer Ctr*., 653 F. Supp. 3d 359, 371 (S.D. Tex. 2023).

[3] Plaintiffs allege that the Website provides for online scheduling (Compl. at ¶ 3), however that allegation is contradicted by the Website itself which is incorporated by reference and which states when a user clicks on a "schedule eye exam" link "[t]his link is taking you to a site outside of Eyemart Express." *See* **Exhibit A**, App'x 0001-0002.

eyewear products, and Soto accessed the Website in June of 2022 to search for prescription eyewear products. *Id*. at ¶¶ 25-27. None of the Plaintiffs allege they actually purchased any prescription eyewear products, entered prescription information, or scheduled such appointments on the Website. *Id*. All of the Plaintiffs allege they have Facebook profiles which contain personally identifiable information such as real names, personal photos, and locations. *Id*.

The Eyemart Privacy Policy states "[w]e collect personally-identifying information you provide to us in connection with your purchases, requests for services, the creation of a personal user account, any material you may post to our Websites or social media pages, or your participation in surveys on any of our Websites." *Id*. at fn. 29.[4] It further discloses "[w]e use third-party tracking services to track non-personally-identifying information about visitors to our Websites in the aggregate. These third-party services may use JavaScript, pixels, transparent GIF files, and other means to enable us to learn which advertisements bring users to our website." *Id*.

D. Facebook and the Meta Pixel

As explained in the Complaint, Meta does not charge users a subscription fee to create a Facebook or Instagram profile, but instead earns its revenue from selling advertising. *Id*. at ¶ 72, fn. 32. When a user logs into a Facebook or Instagram account, that user agrees to certain policies for that account including the Meta Privacy Policy and Cookie Policy. *Id*. at fn. 47.[5] Pursuant to the Meta Cookie Policy, "Cookies help [Meta] provide, protect and improve the Meta Products, such as by personalizing content, tailoring and measuring ads, and providing a safer experience. The cookies that [Meta] use[s] include session cookies, which are deleted when you close your

[4] A true and accurate copy of that Eyemart Privacy Policy, cited by Plaintiffs, is attached hereto as **Exhibit B**, App'x 0003-0018.

[5] Eyemart's cited excerpts from a true and accurate copy of the Meta Privacy Policy, cited by Plaintiffs, is attached hereto as **Exhibit C**, App'x 0019-0028.

browser, and persistent cookies, which stay in your browser until they expire or you delete them." *Id*. Facebook users are assigned a User ID ("UID") number which can be stored on a user's device for up to a year, per Meta's Cookie Policy. *Id*. at ¶ 90. "Any person, even without in depth technical expertise, can utilize the UID to identify owners of the UID via their Facebook profile." *Id*. at 92. Plaintiffs each are alleged to have created Facebook accounts in which Plaintiffs provided Facebook with their real names, locations, photos, and genders. *Id*. at ¶¶ 25-27. When Plaintiffs logged into their Facebook accounts, Plaintiffs were each assigned a UID "automatically" by Meta. *Id*. at ¶ 90.

The Meta Pixel is a piece of code which can be added to a website to measure the effectiveness of advertising by better understanding the actions individuals take on that website. *Id*. at fn. 34. An April, 2022 study found that 80 percent of all internet users encountered the Meta Pixel on websites they visited. *Id*. at ¶ 95, fn 52.[6] More than thirty percent of popular websites have the Meta Pixel installed. *Id*. Meta has transparency tools which allow Facebook users to see what websites have sent information about the user's activities on those websites to Meta. *Id*.

Eyemart has implemented the Meta Pixel on certain sections of the Website. *Id*. at ¶ 90. The use of the Meta Pixel on the Website is publicly disclosed in the Website's background code. *See, e.g.*, Complaint Figures 1-9 (publicly available information gathered by Plaintiffs' counsel showing information tracked through the Meta Pixel on the Website). When a pixel (such as the Meta Pixel) detects an "event" (*i.e.*, a user clicking on a particular button on the Website), that information is sent to the pixel creator (in this case, Meta) through a HTTP request. *Id*. at ¶¶ 93-

[6] A true and accurate copy of that article, Mattu, Surya, *et al*., How We Built a Meta Pixel Inspector, The Markup (April 28, 2022), *available at* https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (last accessed May 6, 2024) cited by Plaintiffs, is attached hereto as **Exhibit D**, App'x 0029-0042.

95. An HTTP request is "a copy of the webpage data" which "if approved, causes the server to send a HTTP Response" and sends those webpage files. *Id*. at ¶ 51.

Thus, the order of operations for websites[7] which have the Meta Pixel installed are as follows: (1) a user on the website interacts on the website in some defined way creating an "event"; (2) the "event" results in a "HTTP request" which is the user's computer sending the website's server a request for the website to act a certain way; (3) the website's server approves the "HTTP request" and sends back an "HTTP response" which results in the website's server sending files to the user based on the user's "HTTP request"; (4) additionally, the Meta Pixel causes a copy of the user's "HTTP request" and the website's "HTTP response" to be sent to Meta; (5) Meta's technology automates analysis of this information, and provides that analysis to the website's operator to generally improve websites based on user interactions on the website. *Id*. at ¶¶ 51, 93, fn. 48, 95, 110, 134-136.

The contents of messages between consumers and companies are regularly, without notice, shared with third parties. *Id.* at 56. Meta has transparency tools which allow Facebook users to see what websites have sent information about the user's activities on those websites to Meta. *Id.* at ¶ 95, fn. 52. Internet users have the option of protecting personal information and online identities through, among other things, use of proxy servers or use of virtual private networks ("VPNs"). *Id*. at fn. 24. "Using a VPN prevents you from leaving footprints on the web." *Id*. There are also publicly available tools and internet browser extensions which "block[] network requests made by

[7] Note, the Meta Pixel is not necessarily on an entire website, but instead is often only on certain sections or pages of a website. Compl. ¶ 85. Each page of a website has a different HTML code, which is how the website's server communicates to a user's computer how that website page should appear and its associated functionalities. *Id*. at ¶¶ 46-47. For ease of reference, this Memorandum does not distinguish between a website having the Meta Pixel installed on certain pages of the website, versus the Meta Pixel being installed on every page of the website.

the Meta Pixel on sites other than Facebook itself, preventing Meta from associating information about a user's activity on websites outside Facebook to that user's Facebook identity." *Id*. at ¶ 95, fn 52. Contrary to these alleged facts and documents incorporated by reference, Plaintiffs claim that they did not know, and could not have known, that details regarding their usages of the Website were disclosed to third-parties. *Id*. at ¶¶ 164-165.

III. ARGUMENT

A. Rule 12(b)(1) Standard

A federal court only has subject matter jurisdiction to adjudicate cases and controversies. To satisfy Article III, a plaintiff must have standing. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *as revised* (May 24, 2016). A court must dismiss a case if it lacks subject matter jurisdiction. *Stockman v. Fed. Election Comm'n*, 138 F.3d 144, 151 (5th Cir. 1998). A showing of standing requires "(1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision." *Soniat v. Texas Real Estate Comm'n*, 721 F. App'x 398, 399 (5th Cir. 2018) (internal brackets omitted). An injury in fact is an "invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. Of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks omitted).

B. Rule 12(b)(6) Standard

Rule 12(b)(6) requires a court to dismiss an action if a plaintiff fails "to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). While a complaint is only required to have "a short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), a complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the

defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint "demands more than an unadorned, the defendant-unlawfully-harmed-me accusation." *Id*.; *see also Lincoln v. Turner*, 874 F.3d 833, 839 (5th Cir. 2017) (a complaint must include "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.").

C. Plaintiffs Fail to Plead Any Cognizable Injury-in-Fact

Plaintiffs' claims fail at the outset because Plaintiffs lack standing. Plaintiffs' fifty-three-page Complaint only mentions harm five times[8] and never once claims any Plaintiffs were injured. As explained below, Plaintiffs' claims for statutory damages under state and federal wiretapping laws lack any injury-in-fact. As to the common law claims brought in Counts IV to VI, Plaintiffs fail to allege how the alleged Website activity monitoring caused Plaintiffs injury-in-fact.

Other cases have considered bare allegations like Plaintiffs' and found such allegations insufficient to support Article III standing. In *In re: BPS Direct, LLC*, users brought a lawsuit against certain sporting goods providers for alleged improper tracking and disclosure of users' online firearm purchases. No. 22-CV-4709, 2023 WL 8458245 (E.D. Pa. Dec. 5, 2023). The matter was dismissed for lack of standing because what was alleged to have been observed on the websites "is no different than what Bass and Cabela's employees would have been able to observe if Website Users had gone into a brick-and-mortar store and began browsing the inventory. Website Users do not have a personal privacy interest in their shopping activity." *Id*. at *12. Further, "[t]he disclosure of [a] Facebook Website User['s] Facebook ID *to Facebook* is hardly intrusive." *Id*. at

[8] Compl. at ¶¶ 20 (stating Plaintiffs "have been harmed" without specifying what that harm is), 30 (claiming the unspecified harms occurred in Texas), 121, 125 (alleging the "site" of the unspecified harm is the device used by the user); and 222 (claiming class members will suffer unspecified harm in the future).

*19 (emphasis in original). *See also Cook v. GameStop, Inc.*, No. 2:22-CV-1292, 2023 WL 5529772, at *4 (W.D. Pa. Aug. 28, 2023), *appeal filed*, No. 23-2574 (3d Cir. Aug. 29, 2023) (holding that a plaintiff "doesn't have a reasonable expectation of privacy in this kind of public shopping behavior in the physical world, and she doesn't have it in the digital world, either.").

As explained above, Plaintiffs agreed to the sharing of information between Meta and Eyemart. Even when accepting all of Plaintiffs' allegations as true, Plaintiffs fail to allege injury in fact required to confer standing to sue in federal court, and Plaintiffs' claims should be dismissed on that basis alone.

D. Eyemart Cannot "Eavesdrop" on Communications Eyemart is a Party To

To state a claim under the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2510, *et seq.*), a plaintiff must plead facts showing that a defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device." *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 274 (3d Cir. 2016). Plaintiffs have not plead that any communication from Plaintiffs to Eyemart has been "intercepted" by Eyemart.

The ECPA is a one-party consent statute. *In re Nickelodeon*, 827 F.3d at 275 (discussing "one party consent language in the Wiretap Act"). Eyemart cannot be found liable for "eavesdropping" on communications directed to Eyemart. *Id.* (dismissing ECPA claim because defendant "was either a party to all communications with the Plaintiff's computers or was permitted to communicate with the Plaintiff's computers by Viacom, who was itself a party to all such communications."); *In re Google Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 142–143 (3rd Cir. 2015) (dismissing ECPA claim because tracking cookies placed by advertising providers made the advertiser the intended recipient of the electronic transmission); *Katz-Lacabe v. Oracle America, Inc.*, 668 F. Supp. 3d 928, 945 (N.D. Cal. 2023) ("As Defendant's

customers must have chosen to deploy Oracle's tools on their websites, it necessarily follows that one of the parties to the communication'—the websites themselves—gave 'prior consent to such interception.'"); *Allen v. Novant Health, Inc.*, 2023 WL 5486240, at *4 (M.D.N.C. Aug. 24, 2023) ("mere receipt of a communication does not constitute a violation").

Similarly, the Missouri wiretap statute also requires the consent of only one of the parties to the communication, foreclosing Plaintiffs' claims based on Missouri law. *Phillips v. Am. Motorist Ins. Co.*, 996 S.W.2d 584, 588 (Mo. Ct. App. 1999); Mo. Rev. Stat. § 542.402.1. ("It is not unlawful for a person to intercept a communication to which he is a party or where one of the parties to the conversation has consented to the interception"); *Jurgens v. Build.com*, 2017 WL 5277679, at *4 (E.D. Mo. Nov. 13, 2017) ("interception is a necessary element for each type of violation."). As the Missouri wiretap statute is modeled after the federal statute, the reasoning for dismissal under the federal statute is equally applicable under the Missouri statute. *State v. King*, 873 S.W.2d 905, 908 (Mo. Ct. App. 1994) ("Our act was modeled after federal statutes enacted in 1968 and revised in 1986." (citing 18 U.S.C.A. §§ 2510–2521)).

Here, Plaintiffs allege that "[a] Pixel cannot be placed on a website by a third-party without being given access by the website's owner. Thus, Eyemart took the affirmative steps necessary to add the Pixel to its Website." Compl. ¶¶ 88-89. To the extent Plaintiffs' activities constitute "communications" under the federal and Missouri wiretapping statutes, one party to those communications (Eyemart) consented, for which Eyemart cannot be held liable. Counts I and II of Plaintiffs' Complaint should therefore be dismissed.

E. Alleged HIPAA Violations Do Not Overcome One-Party Consent Laws

Plaintiffs attempt to plead around the clear prohibition against bringing wiretapping claims against parties to the communications at issue by claiming the purpose of the recording at issue was to commit a crime or tortious act. *See* Compl. ¶ 203. "The prohibition against recording

[communications] for the purpose of committing any criminal or tortious act, however, is construed narrowly" and "is confined to instances where the recording party intends to use the recording to harm or injure a recorded party, such as to blackmail, threaten, or publicly embarrass the recorded party." *Stark v. United States*, No. 3:16-CV-298-M, 2017 WL 1185278, at *4 (N.D. Tex. Mar. 6, 2017) (quoting *United States v. Jiau*, 734 F.3d 147, 152 (2d. Cir. 2013)). HIPAA does not include any private right of action, from which Plaintiffs can claim criminal intent or tortious activity. *Acara v. Banks*, 470 F.3d 569, 571-72 (5th Cir. 2006) ("Every district court that has considered this issue is in agreement that [HIPAA] does not support a private right of action.").

Additionally, Plaintiffs do not allege that the Meta Pixel was installed on the Website with the motivation to commit a crime or tort, but rather to enhance Eyemart's business. "[A] plaintiff must plead sufficient facts to support an inference that the offender intercepted the communication ***for the purpose of a tortious or criminal act*** that is ***independent of the intentional act of recording***." *In re Google Cookie Placement*, 806 F.3d at 145 (emphasis added); *see also Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010) ("[T]o survive a motion to dismiss, a plaintiff must plead sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is independent of the intentional act of recording.").

Plaintiffs fail to plead such a criminal or tortious purpose here, and Plaintiffs' ECPA claims should be dismissed on that basis just as similar allegations have uniformly been dismissed in similar cases across the country. *See Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021) ("Alleged interceptions fall within the tort or crime exception only where the primary motivation or a determining factor in the interceptor's actions has been to injure plaintiffs tortiously . . . cannot apply where the interceptor's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money"); *In re DoubleClick Inc. Priv. Litig.*, 154 F.

Supp. 2d 497, 514-19 (S.D.N.Y. 2001) ("Courts . . . have consistently ruled that a plaintiff cannot establish that a defendant acted with a 'criminal or tortious' purpose simply by proving that the defendant committed any tort or crime"); *Katz-Lacabe*, 668 F. Supp. 3d at 928 (rejecting crime-tort exception in a similar case).

Further, making the conclusory allegation that Eyemart's actions run afoul of purported criminal laws based on unofficial guidance from the U.S. Department of Health and Human Services' Office for Civil Rights has been rejected by other courts, just as it should be rejected here.[9] As one court recently noted, "[t]he interpretation of IIHI [individually identifiable health information] offered by HHS in its guidance goes well beyond the meaning of what the statute can bear." *Kurowski v. Rush System for Health*, Case No. 22-c-5380, 2023 WL 4707184 at *8 (N.D. Ill. July 24, 2023) ("*Kurowski II*"). The court explained that "[a]gency interpretations – such as the HHS guidance – that are arrived at in a less formal manner (i.e., not in the course of rulemaking and adjudication) do not warrant *Chevron*-style deference." *Id*. at 7 (citing *United States v. Mead Corp*., 533 U.S. 218, 230 (2001); *Christensen v. Harris Cnty*., 529 U.S. 576, 587 (2000) ("Interpretations such as those in opinion letters—like interpretations contained in policy

[9] Even if this guidance provided support for Plaintiffs' criminality claims (it does not), it is guidance which has already been revised by yet further guidance. *Compare* HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information, Office of Health and Human Services (Dec. 1, 2022), *available at* https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html (last accessed May 6, 2024); with Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, Office of Health and Human Services (March 18, 2024), *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed May 6, 2024). There is every possibility this guidance will soon be revised again, by the agency or a court of law. Indeed, this guidance is currently being challenged in a lawsuit in this very District. *See Am. Hosp. Ass'n v. Dep't of Health & Human Servs*., Case No. 4:23-cv-01110 (N.D. Tex. Nov. 2, 2023) (lawsuit brought by various healthcare providers against the Department of Health challenging the aforementioned unofficial guidance under the Administrative Procedures Act).

statements, agency manuals, and *enforcement guidelines*, all of which lack the force of law—do not warrant *Chevron*-style deference.") (emphasis in original).

Plaintiffs fail to plead, with the level of particularity required under Rule 9 or otherwise, that Eyemart's incorporation of the Meta Pixel on the Eyemart Website was done for the purpose of committing a crime or tort. Instead, Plaintiffs' allegations are that Meta designed the Meta Pixel and Eyemart implemented the Meta Pixel on the Eyemart Website to enhance its business through advertising. These allegations fall well short of what is required for Plaintiffs to avoid otherwise applicable one-party consent rules. Counts I and II should therefore be dismissed.

F. The Information Sent to Meta Is Not Sent Contemporaneously

All three of the wiretap statutes cited by Plaintiffs require the communication at issue to be wiretapped while the communication is occurring. 720 ILCS 5/14-2(a); Mo. Rev. Stat. § 542.400.6; 18 U.S.C. § 2511(3)(a); *Forsyth v. Barr*, 19 F.3d 1527, 1543 (5th Cir. 1994) ("An 'interception' requires participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device. No new and distinct interception occurs when the contents of a communication are revealed through the replaying of a previous recording." (quoting *United States v. Turk*, 526 F.2d 654, 658 (5th Cir.), *cert. denied*, 429 U.S. 823, 97 S.Ct. 74, 50 L.Ed.2d 84 (1976)). As explained by another court:

> In other words, these statutes give "intercept" its common meaning, which is perhaps best understood through a football analogy. In American football, a ball can only be intercepted when it is "in flight." Once a pass receiver on the offensive team has caught the ball, the window for interception has closed, and defenders can only hope to force a fumble. In essentially the same way, a qualifying "intercept" under the ECPA… can only occur where an e-mail communication is accessed at some point *between* the time the communication is sent and the time it is received by the destination server, at which point it becomes a 'stored communication' within the meaning of the [statute]."

Glob. Pol'y Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) (emphasis added). Here, per Plaintiffs' own Complaint, although the time between Plaintiffs transmitting information

to Eyemart and that same information being transmitted to Meta is slight, the two transmissions are not contemporaneous. *See* Compl. ¶¶ 110, 123, 199 (discussing the "nearly instant[]" duplication of information that is transmitted).

As set forth in the Complaint, when Plaintiffs use the Website, they send information to the servers which host the Eyemart Website which are sorted through "event triggers" such as clicking on links or entering a search into the search bar. Compl. ¶ 93. That information is then sent to Meta's servers through an HTTP request which is automated by the Meta Pixel. *Id*. at ¶ 95. Plaintiffs' Complaint acknowledges that there is no direct "interception" but rather *after* Eyemart receives the information, the information is (in the football terminology) handed off to Meta after reception by Eyemart. *See Fraser v. Nationwide Mut. Ins. Co*., 352 F.3d 107, 114 (3d Cir. 2003) (concluding that company did not intercept employee's e-mail by accessing messages stored on company server).[10]

Other courts that have considered this issue in the Meta Pixel context have ruled similarly. *See Barbour v. John Muir Health*, No. C22-01693, 2023 WL 2618967, at *5 (Cal. Super. Ct. 2023) (dismissing claim against healthcare provider because "the duplication and sending of Facebook's secret code happens after the request reaches its destination" and thus the "Plaintiffs have not alleged Defendant's 'interception' while 'in transit'"); *Licea v. Cinmar, LLC*, 2023 WL 2415592, at *9 (C.D. Cal. Mar. 7, 2023) (dismissing claim "because Plaintiffs do not adequately allege that

[10] This makes sense within the plain meaning of the statutes, *i.e.*, that an entity can pass along information it receives from consumers to third parties without being considered a "wiretapper." If, for example, Plaintiffs sent an email to Eyemart asking about "Nike glasses" or "optometrists near me," there is nothing violative of any statute if that email were to be forwarded to Meta manually or automatically. The fact that a functional equivalent happens through the Website's servers instead of email servers does not turn online exchanges of information with third-parties into wiretapping violations. Nor can it transform a two-step sequence as alleged in the Complaint into a one-step simultaneous event constituting "wiretapping."

their conversations were intercepted in transit"). This Court should therefore dismiss Counts I to III for failure to state a claim.

G. Plaintiffs Consented to Tracking at Issue

Consent to recording of communication is a complete defense to all of Plaintiffs' improper recording claims. *Bliss v. CoreCivic, Inc.*, Case No. 2:18-cv-01280-JAD-EJY, 2024 WL 167149, at *3 (D. Nev. Jan. 16, 2024) ("Consent is a complete defense to claims under the Federal and Nevada Wiretap Acts."); *Cook Au Vin, LLC v. Mid-Century Insurance Company*, 226 N.E.3d 694, 701 (Ill. App. Ct. 1st Dist. 2023) ("The plain language of the [Illinois] eavesdropping statute, however, requires consent only if the eavesdropping device is used in a *surreptitious* manner to record a *private conversation*."(emphasis in original)); Mo. Rev. Stat. § 542.402.1. ("It is not unlawful for a person to intercept a communication to which he is a party or where one of the parties to the conversation has consented to the interception").

Here, Plaintiffs' Complaint demonstrates that Plaintiffs consented to the web tracking they now take issue with. Plaintiffs all allege they are Facebook subscribers who created Facebook profiles. Compl. at ¶¶ 25-27. As stated in the documents incorporated by reference in the Complaint, by utilizing the Facebook product, Plaintiffs agreed to, among other things, the Meta Privacy Policy. *Id.* at ¶ 90, fn. 47. That Privacy Policy states, in part:

> Advertisers, app developers, and publishers and other partners can send us information for business purposes including through the Meta Business Tools they use, our social plugins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities on and off our products—including information about your device, websites you visit, apps you use, games you play, and purchases you make. We also receive information about your online and offline actions, and purchases from third-party data providers who have the rights to provide us with your information. These partners collect your information when you visit their websites or use their services or through third parties they work with.

Id. Plaintiffs cannot agree to allow Meta to track their online activities at websites like Eyemart's Website and then complain of unconsented "injury" when Meta tracks their online activities at Eyemart's Website.

Additionally, the tracking at issue is disclosed in the Eyemart Privacy Policy.[11] As alleged in the Complaint, Meta (not Eyemart) creates and stores the "c_user" cookie on Plaintiffs' devices for up to a year. *Id*. at ¶ 90. Meta (not Eyemart) links that cookie to a Facebook UID. *Id*. Eyemart is not sharing any identifying information to Meta—Meta already has that information by the nature of the individual creating a Facebook account and consenting to Facebook placing a "c_user" cookie on Plaintiffs' devices for up to a year. *Id*. Instead, what Eyemart provides Meta is information regarding, essentially, when buttons are clicked on the Eyemart Website. *Id*. at ¶ 107. If not for the Facebook "c_user" cookie which Plaintiffs agreed to be placed on their own devices, these are "anonymous, limited to usage and volume statistics, and are used to provide insight into the effectiveness of our online marketing initiatives and strategies" as stated in the Eyemart Privacy Policy. *Id*. at ¶ 59, fn. 29.

Plaintiffs' allegations are the digital equivalent to Plaintiffs handing a physical printout of their Facebook account to a Meta employee while Plaintiffs are in an Eyemart store and then complaining that Meta knew Plaintiffs were at an Eyemart store. If Plaintiffs' personally

[11] Plaintiffs barely mention Eyemart's Privacy Policy and instead predicate their contract theory on the statutorily mandated HIPAA privacy notice. However, federal courts have consistently ruled that a HIPAA mandated privacy notice does not constitute an enforceable contract. *See J.R. v. Walgreens Boots All., Inc*., 470 F. Supp. 3d 534, 559 (D.S.C. 2020), aff'd, No. 20-1767, 2021 WL 4859603 (4th Cir. Oct. 19, 2021) ([Notice of Privacy Practices] cannot create contractual obligations because entities like Walgreen[s] Co. are required by law to comply with HIPAA without receiving consideration from plaintiffs.). *See also Brush v. Miami Beach Healthcare Grp. Ltd*., 238 F. Supp. 3d 1359, 1367 (S.D. Fla. 2017) (dismissing breach of contract claim, stating, "[b]ecause the Defendants are required by law to adhere to HIPAA without receiving any consideration from the Plaintiff or any other patient, these provisions cannot create contractual obligations").

identifiable information was disclosed to Meta, it was through the actions of Plaintiffs and Meta, not Eyemart. Counts I-III should therefore be dismissed.

H. Plaintiffs Fail to Plead Contents of Communications with Particularity

Plaintiffs' vague allegations that they visited the Website to "search for prescription eyewear products" or "locate an eye doctor" fall far short of the particularity required under *Twombly*. Plaintiffs do not allege, for example, that any specific test results, diagnoses, or sensitive messages were intercepted or improperly disclosed so as to put Eyemart on notice as to the alleged misconduct. *See e.g., Murphy v. Thomas Jefferson University Hospitals, Inc*., No. CV 22-4674, 2023 WL 7017734, at *6 (E.D. Pa. Oct. 10, 2023) ("without more information about the contents of [p]laintiffs' communications and the parties to whom those contents were disclosed against [p]laintiffs' wishes, their allegations that [defendant's] conduct was 'highly offensive' similarly fall short of the mark" required to bring a common law privacy claim).

Under Counts I to IV, Plaintiffs are required to plead the contents of the communications which Plaintiffs allege were improperly intercepted. Plaintiffs fail to do so here, and Counts I to IV should be dismissed.

I. Plaintiffs Fail to Plead a Claim under the Illinois Eavesdropping Statute

As an initial matter, as set forth above in Section III(F), Plaintiffs' claim fails as there was no "interception" of any private communication. The copying and transmitting of information to Meta happens sequentially and, as a result, does not amount to interception.

Here, to the extent there was any "communication," Eyemart was a party to it, and thus, there can be no violation of the Eavesdropping Act. *See Zak v. Bose Corp*., Case No. 17-cv-02928, 2020 WL 2762552, at *3 (N.D Ill. May 27, 2020) (dismissing claim for violation of Illinois Eavesdropping Act, with prejudice, for failing to allege that defendant was not party to communication); *see also* 720 ILCS § 5/1 2(a)(3); *Vasil v. Kiip, Inc*., 2018 WL 1156328 (N.D. Ill.

Mar. 5, 2018) (dismissing Illinois Eavesdropping Act claim because it does not preclude a party to a communication from recording or transcribing it).

Additionally, the IEA claim is deficient because, even if there was an interception of a communication to which Eyemart was not a party, such interception was not "surreptitious." The IEA defines "surreptitious" as "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS 5/14-1(g). Any information collected through pixels on the Eyemart Website was done with full disclosure in its privacy statement, which Plaintiffs knew about and incorporated by reference into their Complaint.

Finally, the transfer of information regarding Plaintiffs' actions on the Eyemart Website were not transferred surreptitiously. That type of transfer at issue in this case was disclosed in the Eyemart and Meta privacy policies. *See* Compl., ¶¶ 59, fn. 29, 90, fn. 47. It is well known, as documented in Plaintiffs' documents incorporated by reference into the Complaint (*see* Section III(K) below) that this type of web tracking is a common practice by Meta and businesses advertising on Meta. Compl., fn. 6, 33, 34, 36-39, 41-48, 50-52, 55, 58-59, 62-67, 73, and 75-76. Plaintiffs' IEA claim is unsupported by facts or law, and Count III should be dismissed.

J. Plaintiffs Fail to Allege What Contract Terms Were Breached

Plaintiffs also bring common law claims for breach of implied contract and breach of express contract. Under Illinois law, the elements of an implied and express contract are the same: offer, acceptance, and consideration. *Nissan N. Am., Inc., v. Jim M'Lady Oldsmobile, Inc*., 486 F.3d 989, 996 (7th Cir. 2007). "As in physics, two solid bodies cannot occupy the same space at the same time, so in law and common sense, there cannot be an express and implied contract for the same thing, existing at the same time." *In re VTech Data Breach Litigation*, No. 15 CV 10889, 2018 WL 1863953, at *3 (N.D. Ill. Apr. 18, 2018) (citations omitted). Colorado and Missouri law require a similar meeting of the minds to form an enforceable contract. *Cayo, Inc. v. Swiss*

Reinsurance Am. Corp., No. 23-CV-00105-MEH, 2023 WL 4744196, at *9 (D. Colo. May 2, 2023); *Nickel v. Stephens Coll.*, 480 S.W.3d 390, 397 n.6 (Mo. Ct. App. 2015).

Noticeably missing from the Complaint are any specific terms of any agreement between Eyemart and Plaintiffs that Eyemart allegedly breached. Instead, Plaintiffs make the conclusory allegations that by merely providing information to Eyemart, some sort of enforceable contract was formed which prohibited Eyemart from sharing that information with Meta. Compl. ¶¶ 254-255. Plaintiffs further allege that, despite earlier pleading that "the Terms of Use are quiet as to the handling of [Plaintiffs' information]" (*id*. at ¶148) that somehow those same Terms of Use "include the promise to protect nonpublic personal information given to Eyemart or that Eyemart gathered on its own, from disclosure." *Id*. at ¶ 262. Plaintiffs do not even allege they read or relied upon the Terms of Use which Plaintiffs claim to be "quiet as to the handling of [Plaintiffs' information]," *see Willingham v. Glob. Payments, Inc*., Case No. 1:12–CV–01157, 2013 WL 440702, at *20 (N.D. Ga. Feb. 5, 2013) ("broad statements of reliance on a defendant's website and privacy statement do not give rise to contract claims where, as here, Plaintiffs do not allege that they read and relied upon those statements").

Plaintiffs' contractual allegations, again, do not meet the particularity requirements under federal or state law, and the Court should dismiss Counts V and VI accordingly.

K. Plaintiffs Fail to Allege a Plausible Factual Basis for Their Alleged Expectations of Privacy

Plaintiffs fail to state a claim for "intrusion upon seclusion." Under Colorado and Illinois law, a claim of intrusion upon seclusion requires the intrusion to be to be of something "private" and of such a nature to be highly offensive or objectionable to a reasonable person. *Smith v. City of Chicago*, 143 F. Supp. 3d 741, 761 (N.D. Ill. 2015); *Quigley v. Rosenthal*, 327 F.3d 1044, 1073 (10th Cir. 2003). Missouri law requires the information obtained to be "of a secret and private

subject matter." *Thomas v. Corwin*, 483 F.3d 516, 531 (8th Cir. 2007) (citing *St. Anthony's Med. Ctr. V. H.S.H.*, 974 S.W.2d 606, 609–10 (Mo. Ct. App. 1998)).

Throughout the Complaint, Plaintiffs make the conclusory allegation that their interactions on the Website are "inherently private" and that they "reasonably expected" these interactions to be private without providing any plausible factual basis for those allegations. Plaintiffs' alleged reasonable expectation of privacy certainly could not have come from Meta's disclosures about the information it receives and uses. Compl., fn. 6, 33, 34, 36-39, 41-48, 50-52, 55, 58-59, 62-67, 73, and 75-76. It could not have come from the Eyemart Privacy Policy, which expressly discloses the use of "third-party tracking services to track non-personally-identifying information about visitors to our Websites" including use of "JavaScript, pixels, transparent GIF files, and other means" *Id*. at ¶ 59, fn. 29. This expectation of privacy cannot be derived from the over seventy-five footnotes and associated materials incorporated by reference into the Complaint, many discussing all the ways Meta discloses its Meta Pixel functionalities and the proliferations of tracking throughout the internet. *Id*. at fn. 1-76.

If Plaintiffs truly believed their Website visits and searches were of a highly confidential nature, they fail to explain why they entered information on a public website while failing to avail themselves of the plethora of online privacy preserving technologies described in documents incorporated by reference in the Complaint like ad blockers, browser extensions, or VPNs. *Id*. at fn. 24.

As another district court recently held when addressing nearly identical claims involving the Meta Pixel, "the collection and disclosure of a user's browsing history and personal information on a public website is 'routine commercial behavior' and not 'highly offensive.'" *Cousin v. Sharp Healthcare*, No. 22-cv-2040-MMA, 2023 WL 4484441, at *6 (S.D. Cal. July 12,

2023); *see also* Compl. ¶ 56 (stating the contents of messages between consumers and companies are regularly, without notice, shared with third parties).

It is also unclear what facts Plaintiffs rely on for the claim that searching for information on a public website carries with it any expectation of privacy. Plaintiffs' cited exemplars of this claimed "highly offensive" information sharing include: (1) searching for Nike sunglasses on a public website and (2) locating eyewear stores locations on a public website. *See* Compl., pg. 22-23. Plaintiffs provided that information to Eyemart. *Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 342-43 (E.D. Pa. 2012) (dismissing intrusion claim, stating, "liability for intrusion upon seclusion cannot exist where a defendant legitimately obtains information from a plaintiff . . . This is so even where those facts voluntarily offered are later disclosed to a third party, even by . . . newspaper publication").

Plaintiffs' examples are not protectable private information. Meta is getting no more information from the tracking alleged in Plaintiffs' Complaint than if the same individual, while logged into Facebook on their browser, also searched for that information elsewhere online such as on Amazon or Reddit or WebMD or any number of other third-party sites which are not medical care providers. *In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d 968, 973, 987-88 (N.D. Cal. 2014) (finding any intrusion regarding a web user's "identifying information, browsing habits, search queries" not highly offensive, stating that there is a "a high bar for the requisite intrusion that is highly offensive to a reasonable person").

Plaintiffs entered information into a public website without any agreement that such information would not be recorded and shared. If Plaintiffs expected that the information they entered into a public website would be kept confidential, that expectation was not reasonable and

is not supported by non-conclusory plead facts or the law. The Court should dismiss Count IV of the Complaint.

IV. CONCLUSION

Plaintiffs made the choice to take advantage of Meta's free social media services in exchange for providing Meta access to certain data for Meta to monetize. Plaintiffs chose to visit the publicly available Eyemart Website, which disclosed its use of third-party pixel providers like Meta. Plaintiffs chose to enter information into that public Website, after making their agreements with Meta, and with knowledge of the Website's tracking functionalities. Plaintiffs cannot now claim damages for the data collection at issue.

Plaintiffs' Complaint should be dismissed for lack of standing. The Complaint should additionally be dismissed with prejudice for failure to state a claim upon which relief may be granted. "A dismissal with prejudice is appropriate when amending a complaint would be futile." *Taubenfeld v. Hotels.com*, 385 F. Supp. 2d 587, 592 (N.D. Tex. 2004) (citing *Schiller v. Physicians Res. Group, Inc.*, 342 F.3d 563, 566 (5th Cir. 2003)). As stated above, no amendment can change the technical realities which make the information transmission at issue in this case fall outside the "contemporaneous" requirements of wiretapping statutes. Nor can Plaintiffs submit new pleadings which allege the facts necessary under the law showing their use of a public website entitles them to a plausible claim of relief.

WHEREFORE, for the foregoing reasons, Eyemart Express LLC respectfully requests this Court dismiss the Complaint with prejudice and render any and all further relief which this Court deems just and proper.

Dated: May 6, 2024

By: */s/ Andrew F. Newman*
Andrew F. Newman
Texas State Bar No. 24060331
POLSINELLI PC
2950 N. Harwood Street, Suite 2100
Dallas, Texas 76005
Tel: (214) 661-5506
Fax: (214) 397-0033
Email: afnewman@polsinelli.com

John C. Cleary (*pro hac vice forthcoming*)
New York Bar No. 1969146
POLSINELLI PC
600 Third Avenue, 42nd Floor
New York, NY 10016
Tel: (212) 413-2837
Fax: (212) 684-0197
Email: john.cleary@polsinelli.com

Jonathan E. Schmalfeld (*pro hac vice forthcoming)*
Missouri Bar No. 68374
POLSINELLI PC
7676 Forsyth Boulevard, Suite 800
St. Louis, MO 63105
Tel: (314) 622-6621
Fax: (314) 231-1776
Email: jschmalfeld@polsinelli.com

ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

The undersigned certifies that on May 6th, 2024, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document through the Court's CM/ECF system. Any other counsel of record will be served by a facsimile transmission and/or first-class mail.

Andrew F. Newman
Andrew F. Newman